

# Modeling Internet Security Investments

## *The Case of Dealing with Information Uncertainty*

Ranjan Pal and Pan Hui

University of Southern California, Deutsch Telekom Laboratories

Email: rpal@usc.edu, pan.hui@telekom.de

### Abstract

Modern distributed communication networks like the Internet and censorship-resistant networks (also a part of the Internet) are characterized by nodes (users) interconnected with one another via communication links. In this regard, the security of individual nodes depend not only on their own efforts, but also on the efforts and underlying connectivity structure of neighboring network nodes. By the term ‘effort’, we imply the amount of investments made by a user in security mechanisms like antivirus softwares, firewalls, etc., to improve its security. However, often due to the large magnitude of such networks, it is not always possible for nodes to have complete effort and connectivity structure information about all their neighbor nodes. Added to this is the fact that in many applications, the Internet users are selfish and are not willing to co-operate with other users on sharing effort information. In this paper, we adopt a non-cooperative game-theoretic approach to analyze individual user security in a communication network by accounting for both, the partial information that a network node possess about its underlying neighborhood connectivity structure, as well as the presence of positive externalities arising from efforts exerted by neighboring nodes. We investigate the equilibrium behavior of nodes and show 1) the existence of symmetric Bayesian Nash equilibria of efforts and 2) better connected nodes choose lower efforts to exert but earn higher utilities with respect to security improvement *irrespective* of the nature of node degree correlations amongst the neighboring nodes. Our results provide ways for Internet users to appropriately invest in security mechanisms under realistic environments of information uncertainty.

*Keywords:* security, externality, Bayesian Nash Equilibria

### I. INTRODUCTION

The Internet has become a fundamental and integral part of our daily lives. Billions of people are using the Internet for various types of applications that demand different levels of security. For example, commercial and government organizations run applications that require a high level of security, since

security breaches would lead to large financial damage and loss of public reputation. Another example of a high security application in the Internet is maintaining user anonymity through a censorship-resistant network. On the other hand, an ordinary individual for instance generally uses a computing device for purposes that do not demand strict security requirements. However, all these applications are running on a network, that was built under assumptions, some of which are no longer valid for today's applications, e.g., that all users on the Internet can be trusted and that the computing devices connected to the Internet are static objects. Today, the Internet comprises of both good and malicious users. The malicious users perform illegal activities, are able to aspect many users in a short time period, and at the same time reduce their chances of being discovered. To overcome security related issues, Internet users invest in security mechanisms such as anti-virus solutions and firewalls.

It is commonsense information that due to Internet connectivity, the security strength of an Internet user<sup>1</sup> is dependent on the security strength of other users, especially neighboring users. Thus, from an individual user perspective, two important pieces of information are the amount of security investments of its neighbors in the network and the knowledge of the underlying connectivity structure of its neighbors, as they both drive optimal user investments. Unfortunately, due to the large magnitude of the Internet, its not feasible or practical to have exact information about the security investments and connectivity structure of all neighboring Internet users. In addition, most Internet users are selfish in nature and would not be inclined to share investment information with other Internet users. However, users do need to invest in security/defense mechanisms to protect themselves as much as possible. In this paper, we address the problem of optimal security investments when an individual user is uncertain about the underlying network connectivity structure of its neighbors , and accounts for the network externalities<sup>2</sup> posed by them when they invest in security mechanisms.

We consider models related to two general security scenarios as mentioned in [15] when network externalities are present: 1) where the security strength of an individual user depends upon the sum security strength of itself and other individual nodes in the network under operation and 2) where the security strength of an individual user depends on the strength of the strongest node/s in the network. An example of scenario 1 is a peer-to-peer network where an attacker might want to slow down the transfer of a given piece of information, whose transfer speed might depend on the aggregate effort of

<sup>1</sup>An Internet user could be a single individual or an individual organization.

<sup>2</sup>An externality is a positive(negative) effect caused to a user not directly involved in an economic transaction, by other users involved in the transaction. For example, an Internet user investing in security mechanisms benefits all the nodes connected to it and thus creates a positive externality for its neighbors.

all relevant nodes concerned. An example of scenario 2 is a censorship-resistant network, where a piece of information will remain available to a public domain as long as at least one node serving that piece of information is unharmed. Another example of scenario 2 is the flow of traffic between two backbone nodes in the Internet. Modeling each path between two backbone nodes as a node, traffic will flow securely between the backbone as long as there is at least one node that is unharmed by an attacker, i.e., there exists at least one path between the backbone nodes. Likewise, there are other examples of applications on the Internet that fit scenarios 1 and 2. We emphasize here that there is another practical scenario as mentioned in [15], viz., one where the security strength of an individual user depends on the strength of the weakest node. This scenario is mainly an intra-organization scenario, where once a node in an organization is compromised due to a weak password or a security policy, it is easy for an attacker to hack the whole system. However, the information of neighborhood topology structure within an organization may be known to the network users in certainty, but in this paper we focus on the case when users have uncertain information about the neighborhood topology structure of the network in operation.

#### *Our Research Contributions*

- 1) We present a general model for analyzing individual user security in a non co-operative Internet environment. In this regard, we study security games when 1) Internet users have incomplete information about the underlying neighboring network connectivity structure and 2) Internet users account for the positive externalities posed by the investments of neighboring Internet users. Our model extends work proposed in [5][6] in terms of capturing network information uncertainty. (See Section III.)
- 2) We formulate our investment problem as a Bayesian game of incomplete information and show the existence of a symmetric Nash equilibrium of user investments. The equilibrium results show that under incomplete neighboring network topology information, better connected users choose lower efforts to exert and earn higher payoffs, *irrespective* of the nature of node degree correlations amongst neighboring nodes.<sup>3</sup>. (See Section IV.)

<sup>3</sup>In a network such as the Internet, there exists a correlation between the node degrees [11]. In this paper we explicitly model the degree correlations.

## II. RELATED WORK

There have been very few works related to security investments in the Internet. The authors [9][14] in their works have analyzed self-protection investments in Internet security under the presence of cyber-insurance, which is a form of a third-party risk transfer. Under the assumption of users having complete network topology information, the works show 1) cyber-insurance incentivizes users to invest in self-protection, 2) cyber-insurance entails optimal user investments both in insurance and in self-protection, and 3) co-operation amongst Internet users result in higher user self-protection investments when compared to the case when users do not co-operate. However, attractive though the concept may seem, cyber-insurance may not be a market reality due to factors such as inter-dependent security, correlated risks, and information asymmetry between the insurer and the insured [1][12]. In addition, it is also infeasible for Internet users to have complete network topology information.

For non cyber-insurance environments, in a recent series of works [7][13], the authors show that Internet users invest sub-optimally in security under selfish environments when compared to the case when user co-operation is allowed. They account for externalities but base their results by assuming users having complete network topology information. However, as we have discussed previously, in a large network such as the Internet, having complete network topology information is infeasible. In addition, all the mentioned related works do not model the well-known security games mentioned in [15], that are in general played by attackers and defenders (non malicious Internet users) when externalities are present in a network. In this regard, the works in [4][5][6] tackle the problem of optimal security investments and model the cited security games mentioned in [15] but do not account for any uncertainty of information that a user has regarding the underlying network topology. In this paper, we advance previous research in security investments and model both, externalities, as well as users having uncertainty of information regarding the connectivity structure of neighboring nodes. However, unlike [5][6], we do not model self-insurance, and only focus on self-protection without any cyber-insurance.

## III. MODELING NETWORK SECURITY INVESTMENT GAMES

In this section, we propose a general model for analyzing network security investments using a game-theoretic approach. First, we model the user interaction network in the Internet. Second, we describe the utility/payoff function of the Internet users as a function of their strategies/actions, which are nothing but the security investments of a user. Finally, we explain the information structure of Internet users with

respect to the underlying connectivity structure of their neighbors, and highlight the game of investments that results from the information structure.

### A. Network Structure

We consider a set  $N = \{1, \dots, n\}$  of  $n$  Internet users and a connectivity matrix  $G = (V, E)$  of users, where  $v_{ij} = 1$  if the utility of user  $i$  is affected by the security investment of user  $j$ ,  $i$  being not equal to  $j$ , and 0 otherwise. Let  $N_i(v) = \{j | v_{ij} = 1\}$  denote the set of all the one hop neighbors of  $i$ , where  $v \in \{0, 1\}^{n \times n}$ . We also consider the  $k$ -hop neighbors of node  $i$  and denote the set by  $N_i^k(v)$ . This set consists of all the nodes that are within  $k$ -hops of node  $i$ , where  $k \geq 1$ . Inductively, we have the following relationships between  $N_i^k(v)$  and  $N_i(v)$ :

$$N_i^1(v) = N_i(v). \quad (1)$$

$$N_i^k(v) = N_i^{k-1}(v) \cup (\cup_{j \in N_i^{k-1}(v)} N_j(v)). \quad (2)$$

We represent the degree of a node  $i$  by  $d_i$ , where  $d_i$  equals  $|N_i(v)|$ . In this paper, we assume that each user has perfect knowledge about its own degree but does not have complete information about the degrees of its neighbors. (More on degree information structure in Section III-C.)

### B. User Strategies and Payoffs

In this paper we consider two types of non co-operative security investment games concerning the case when users have incomplete information on the topology of the network under operation: (1) the users are selfish and invest to maximize their own utilities, but the security strength of an individual user depends on the sum of security investments of itself and its neighboring individual nodes and 2) the users are selfish and invest to maximize their own utilities, but the security strength of the whole network depends on the security investments of the most robust node/s amongst its neighbors. The latter type of game is often termed as a ‘best-shot’ game. In both these types of games, each user is a player and its strategy is the amount of security investment it makes. We assume here that the strategy/action of each user  $i$  is  $x_i$  and lies in the *compact*<sup>4</sup> set  $[0, 1]$ . We also assume that the utility/payoff to each user  $i$  is  $U_i$  and is a function of the security investments made by itself and its one hop neighbors. Thus  $U_i = U_i(x_i, \vec{x}_{N_i(v)})$ , where  $\vec{x}_{N_i(v)}$  is the vector of security investments of the one hop neighbors of user  $i$ . From the structure

<sup>4</sup>In mathematical analysis, a compact set is one which is closed and bounded.

of user utility functions, we observe that two players having the same degree will have the same utility function. We also model the concept of a positive externality as it forms an integral part of the analysis in Section IV. A positive externality to a user from its one hop neighbors results when they invest in security, thereby improving the individual security strength of the user. We represent the concept mathematically in the following manner: we say that a payoff function exhibits positive externalities if for each  $U_i$  and for all  $\vec{x} \geq \vec{x}'$ ,  $U_i(x_i, \vec{x}) \geq U_i(x_i, \vec{x}')$ , where  $\vec{x}$  and  $\vec{x}'$  are the vectors of security investments of one hop neighbors of user  $i$ .

In scenarios where the security strength of a user  $i$  depends on the sum of investments of itself and other neighboring users, we mathematically formulate  $i$ 's utility/payoff function as follows:

$$U_i(x_1, \dots, x_{d_i}) = f\left(x_i + \lambda \sum_{j=1}^{d_i} x_j\right) - c(x_i), \quad (3)$$

where  $f(\cdot)$  is a non-decreasing function,  $c(\cdot)$  is the cost incurred by user  $i$  for putting in own effort in order to make its system more robust, and  $\lambda$  is a scalar quantity which determines the magnitude of the positive externality experienced by user  $i$  due to the security investments made by its one hop neighbors.

The situation when the security strength of a user depends on the investments made by the strongest neighbor/s can be modeled as a special case of the situation when a user security strength depends on the sum of the security investments of its neighbors. We first note that from user  $i$ 's perspective, the former situation implies that as long as there is a neighboring node/s that is secure, user  $i$  is safe. In Section I we have already cited censorship resistant networks and Internet backbone networks to be examples of networks where the former situation might arise leading to a best-shot game. We had also given an example of how the best-shot scenarios arising in these networks can be modeled as a graph to reflect the 'user-neighbor' concept.

Once we have modeled a best-shot scenario as a graph, we fix the strategy space of individual users to  $\{0, 1\}$  and make  $f(0) = 0$  and  $f(y) = 1$  for all  $y \geq 1$ . A binary strategy space of  $\{0, 1\}$  implies that each user decides either to invest or not to invest. If a user or any of its neighbors invest, the former is safe, else it is not. We observe that the 'sum of investments' game gets converted to a best-shot game. In this case user  $i$ 's payoff follows the following equation:

$$U_i(x_i, (\vec{x}, 0)) = U_i(x_i, \vec{x}), \forall (x_i, \vec{x}) \in [0, 1]^{d_i+1}. \quad (4)$$

Equation (4) implies that adding a link to a neighbor who invests zero amount in security mechanisms is

equivalent to not having the neighbor.

### C. Information Structure

In this paper we assume that each Internet user (player) knows its own degree but does not have perfect information regarding the degree of its neighbors. It has already been shown by Newman in [11] that nodes in an Internet like network exhibit degree correlations<sup>5</sup> In this regard, we account for the degree correlations between the neighboring nodes of a user  $i$  in our model, i.e., when a user decides on its strategy, it accounts for the amount of information it has on the degree of its neighbors. Information on degree correlations is important as it guides a user to making better security investments when compared to the situation when it has no information about the correlations.

Let the degrees of the neighbors of user  $i$  be the vector  $\vec{d}_{N_i(v)}$ , whose dimension is  $d_i$ . We assume that user  $i$  does not know the vector  $\vec{d}_{N_i(v)}$  but has information regarding its probability distribution, i.e., it knows the value of  $P(\vec{d}_{N_i(v)}|d_i)$ . We assume that each player in the network under consideration has symmetrical beliefs about the degree of its neighbors. Thus, arises a family of conditional distributions,  $\mathbf{C} \equiv \{[P(\vec{d}|d)]_{\vec{d} \in \mathbb{N}^d}\}_{d \in \mathbb{N}}$ , where  $\vec{d}$  is a vector of degrees of the neighbors of a node and  $d$  is the degree of a given node.

We model the strategic interactions between the players of the network as a *Bayesian game of incomplete information*. The type space of the Bayesian game is the user knowledge on the potential degrees of its neighboring players. The strategy for each player is its security investment conditioned on the knowledge of the degree of their neighbors, and the payoff function for each player is as defined in Section III-B, which depends on whether the game is a sum of investments game or a best-shot game. Assuming that  $S$  is the set of possible investments a user could make, the strategy for player  $i$  is a mapping  $\gamma_i : \{0, 1, \dots, n-1\} \rightarrow \Omega(S)$ , where  $\Omega(S)$  is the set of distribution functions on  $S$ .

We note that for a player, its conditional distributions concerning the neighbors' degrees can vary with its own degree. According to our model, players may have different number of neighbors, and the degrees of the neighbors are correlated with each other. Thus, the dimension of the vector of degrees of its neighbors may vary from player to player. In order to address correlation amongst vectors of different dimensions, we adopt the technique of 'association' from the domain of statistics [3]. Association is used to track the correlation patterns of groups of random variables, given the complicated interdependencies

<sup>5</sup>Newman show through empirical studies that technological and Internet networks exhibit negative degree correlation whereas social networks exhibit positive degree correlation.

that might be present between them. A positive association indicates that higher levels of one variable (in this case a player's degree) implies higher levels of all other variables (in this case a player's neighbors' degrees).

Given a player  $i$  with degree  $d_i$ , enumerate the degrees of  $i$ 's neighbors as  $\vec{d}_{N_i(v)} = (d_1, \dots, d_{d_i})$ . Now consider a function  $F : \{0, 1, \dots, n-1\}^m \rightarrow \mathbb{R}$ , where  $m \leq d_i$ . Let

$$E_{P(\cdot|d_i)}[F] = \sum_{\vec{d}_{N_i(v)}} P(\vec{d}_{N_i(v)}|d_i) F(d_1, \dots, d_m). \quad (5)$$

In Equation (5) we fix a subset  $m \leq d_i$  of user  $i$ 's neighbors, and then take the expectation of  $F$  operating on their degrees. We say that the family of distributions  $\mathbf{C}$  exhibits positive association if, for all  $k' > k$ , and any non-decreasing  $F : \{0, 1, \dots, n-1\}^k \rightarrow \mathbb{R}$ , we have

$$E_{P(\cdot|k')}[F] \geq E_{P(\cdot|k)}[F], \quad (6)$$

and  $\mathbf{C}$  exhibits negative association if

$$E_{P(\cdot|k')}[F] < E_{P(\cdot|k)}[F], \quad (7)$$

for all  $k' > k$ , and any non-decreasing  $F : \{0, 1, \dots, n-1\}^k \rightarrow \mathbb{R}$ .

#### IV. GAME ANALYSIS

In this section, we analyze the *symmetric* Bayesian game of incomplete information played between the users of the network under operation. In any symmetric game, the player payoffs for playing a particular strategy depend only on the strategies of other players and not on who is playing the strategies. We investigate the existence, uniqueness, and monotonicity of our game equilibria. In studying monotonicity of equilibria, we investigate the changes in the best response investment magnitude of a user when other users in the network increase/decrease their best response investment amounts. We also investigate the effect of the increase/decrease in user degrees on the equilibria of the game. We initially give a mathematical definition of our Bayesian game and follow it up with the analysis of game equilibria.

##### A. Game Definition

Consider a player (Internet user)  $i$  having degree  $d_i$  in a *sum-of-investments game* or a *best-shot game*. Each player chooses a security investment amount from the set  $S$  as its strategy, where  $S$  is as defined in



Section III-C. Let  $d\rho_{-i}(\vec{\gamma}, d_i)$  be the probability density over  $x_{N_i(v)} \in S^{d_i}$  induced by the beliefs  $P(\cdot|d_i)$  held by player  $i$  over the degrees of its neighbors, combined with the strategies played via  $\vec{\gamma}$ , the vector of strategies of other users in the network. Let

$$EU_i(x_i, \vec{\gamma}, d_i) = \int_{x_{N_i(v)} \in S^{d_i}} U_i(x_i, x_{N_i(v)}) d\rho_{-i}(\vec{\gamma}, d_i), \quad (8)$$

where  $EU_i(x_i, \gamma, d_i)$  is the expected utility/payoff of player  $i$  with degree  $d_i$  and investment  $x_i$  when other players choose strategy  $\vec{\gamma}$ . The *Bayesian Nash equilibrium* of the game is a strategy vector that *maximizes* the expected utility of each player in the network [2][10]. In regard to individual user expected payoff functions, we now define the concepts of degree complementarity and degree substitutability that will be of importance in the analysis of the *monotonicity* of game equilibria.

For a given player  $i$ , we say that its expected utility function exhibits degree complementarity if

$$EU_i(x_i, \vec{\gamma}, d_i) - EU_i(x'_i, \vec{\gamma}, d_i) \geq EU_i(x_i, \vec{\gamma}, d'_i) - EU_i(x'_i, \vec{\gamma}, d'_i), \quad (9)$$

where  $x_i > x'_i$ ,  $d_i > d'_i$ , and  $\vec{\gamma}$  is non-decreasing. Similarly for a given player  $i$ , we say that its expected utility function exhibits degree substitutability if

$$EU_i(x_i, \vec{\gamma}, d_i) - EU_i(x'_i, \vec{\gamma}, d_i) \leq EU_i(x_i, \vec{\gamma}, d'_i) - EU_i(x'_i, \vec{\gamma}, d'_i), \quad (10)$$

where  $x_i > x'_i$ ,  $d_i > d'_i$ , and  $\vec{\gamma}$  is non-increasing. We have the following lemma and ensuring the conditions under which the expected utility of a player exhibits degree complementarity.

**Lemma 1.** *Given the conditions that (1)  $U_i(x_i, (\vec{x}, 0)) = U_i(x_i, \vec{x})$ ,  $\forall (x_i, \vec{x}) \in [0, 1]^{d_i+1}$ , for each player  $i$ , (2) the  $U_i(\cdot)$ 's for each player  $i$  exhibit strategic complements<sup>6</sup>, and (3) the family of conditional distributions  $\mathbf{C}$  is positively associated, then  $EU_i$ 's for each player  $i$  exhibits degree complements.*

We omit the proof due to lack of space. We emphasize here that the proof structure also establishes that given (1)  $U_i(x_i, (\vec{x}, 0)) = U_i(x_i, \vec{x})$ ,  $\forall (x_i, \vec{x}) \in [0, 1]^{d_i+1}$ , for each player  $i$ , (2) the  $U_i(\cdot)$ 's for each player  $i$  exhibit strategic substitutes, and (3) the family of conditional distributions  $\mathbf{C}$  is negatively associated,  $EU_i$ 's for each player  $i$  exhibits degree substitutes.

<sup>6</sup> $U_i(\cdot)$  is said to exhibit strategic complements [16] if for all  $d_i$ ,  $x_i > x'_i$  and  $\vec{x} \geq \vec{x}'$  implies  $U_i(x_i, \vec{x}) - U_i(x'_i, \vec{x}) \geq U_i(x_i, \vec{x}') - U_i(x'_i, \vec{x}')$ . Analogously,  $U_i(\cdot)$  is said to exhibit strategic substitutes [16] if for all  $d_i$ ,  $x_i > x'_i$  and  $\vec{x} \geq \vec{x}'$  implies  $U_i(x_i, \vec{x}) - U_i(x'_i, \vec{x}) \leq U_i(x_i, \vec{x}') - U_i(x'_i, \vec{x}')$ .

## B. Game Equilibria Results

In this section we state the results related to equilibria of our proposed Bayesian game. Given a symmetric environment; i.e., players participate in a symmetric Bayesian game of security investments, we prefer to analyze *symmetric equilibria*<sup>7</sup>, as asymmetric behavior seems relatively unintuitive, and difficult to explain in a one-shot interaction [8]. We omit the proofs of the results due to lack of space.

**Lemma 2.** *There exists a symmetric equilibrium in our proposed security investment game. If the expected utility function of users exhibit degree complementarity, the equilibrium is non-decreasing, whereas for user utility functions exhibiting degree substitutes, the equilibrium is non-increasing.*

**Lemma 3.** *Given the conditions that (1)  $U_i(x_i, (\vec{x}, 0)) = U_i(x_i, \vec{x})$ ,  $\forall (x_i, \vec{x}) \in [0, 1]^{d_i+1}$ , for each player  $i$  and (2) degrees of neighboring nodes of users are independent, then strategic substitutes (compliments) of user utility functions result in every symmetric equilibrium of our proposed Bayesian game being monotone increasing (decreasing).*

**Lemma 4.** *Suppose  $U_i(x_i, (\vec{x}, 0)) = U_i(x_i, \vec{x})$ ,  $\forall (x_i, \vec{x}) \in [0, 1]^{d_i+1}$ , for each player  $i$ . If  $\mathbf{C}$  is positively associated, then in every non-decreasing symmetric equilibrium of our proposed Bayesian game, the expected utilities of players are non-decreasing in degree. If  $\mathbf{C}$  is negatively associated, then in every non-increasing symmetric equilibrium of our proposed Bayesian game, the expected utilities of players are non-decreasing in degree.*

*Lemma Comments:* From a user (player) perspective, Lemma 2 states that when user expected utilities exhibit degree complementarity, a monotonic increase in the equilibrium security investments of all other users results in an increase in the player's equilibrium investments, for at least one equilibrium. Thus, the degree complementarity property of user expected utilities prevents *free-riding* behavior of users for at least one equilibrium. On the other hand, the degree substitutes property ensures that for at least one equilibrium, users are not incentivized to increase their security investments when others in the network do not, in turn providing no additional benefit to other network users by investing relatively more. Lemma 3 states the conditions under which all symmetric equilibria are monotone, and gives an insight on the topology of the network that could result in all symmetric equilibria being monotone. Lemma 4 provides

<sup>7</sup>A symmetric equilibrium is one where each player in the game plays the same strategy.

the relation between network degrees of users and their equilibrium payoffs, and identifies the conditions under which payoffs increase/decrease with network degree. The relationships state the contexts in which network connections are advantageous and disadvantageous with respect to equilibrium payoffs.

## V. CONCLUSION

In this paper we proposed a security investment model for the Internet in which Internet users account for the positive externality posed to them by other Internet users and make security investments under situations when they do not have complete information about the underlying connecting topology of its neighbors. Our model is based on a game-theoretic approach and we showed 1) the existence of symmetric Bayesian Nash equilibria of efforts and 2) better connected nodes choose lower efforts to exert but earn higher utilities with respect to security improvement *irrespective* of the nature of node degree correlations amongst the neighboring nodes. Our results provided ways for Internet users to appropriately invest in security mechanisms under realistic environments of information uncertainty. Our results also clarified how the basic strategic features of the game - as manifest in the complements and substitutes property - combine with different patterns of degree association to shape network behavior and user payoffs. As a part of future work, we plan to incorporate the network concepts of centrality and clustering in our model in addition to degree distributions. We also plan to investigate security investments under an asymmetric environment, i.e., a game environment in which user payoffs depend not only on the strategy of other users but also on the identity of the users.

## REFERENCES

- [1] R. Bohme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *WEIS*, 2010.
- [2] D.Fudenberg and J.Tirole. *Game Theory*. MIT Press, 1991.
- [3] J. D. Esary, F. Proschan, and W. Walkup. Association of random variables with applications. *Annals of Mathematical Statistics*, 38(5), 1967.
- [4] N. Fultz and J. Grossklags. Blue versus red: A model of distributed security attacks. In *International Conference on Financial Cryptography and Data Security*, 2009.
- [5] J. Grossklags, N. Christin, and J. Chuang. Secure or insure ? a game-theoretic analysis of information security games. In *WWW*, 2008.
- [6] J. Grossklags, N. Christin, and J. Chuang. Security and insurance management in networks with heterogenous agents. In *ACM EC*, 2008.
- [7] L. Jiang, V. Ananthram, and J. Walrand. How bad are selfish inverstments in network security. *To Appear in IEEE/ACM Transactions on Networking*, 2010.
- [8] D. Kreps. *Game Theory and Economic Modelling*. Oxford University Press, 1990.
- [9] M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In *IEEE INFOCOM*, 2009.
- [10] M.J.Osborne and A. Rubinstein. *A Course in Game Theory*. MIT Press, 1994.
- [11] M. E. J. Newman. Assortative mixing in networks. *Phys.Rev.Lett.*, 89, 2002.
- [12] N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand. Competitive cyber-insurance and internet security. In *WEIS*, 2009.
- [13] J. Omic, A. Orda, and P. V. Mieghem. Protecting against network infections: A game theoretic perspective. In *IEEE INFOCOM*, 2009.
- [14] R. Pal and L. Golubchik. Analyzing self-defense investments in the internet under cyber-insurance coverage. In *IEEE ICDCS*, 2010.
- [15] H. Varian. System reliability and free riding. In *ACM ICEC*, 2003.
- [16] H. R. Varian. *Microeconomic Analysis*. Norton, 1992.